Sc

d'Cryptor® SC Cryptographic Module

Non-Proprietary Security Policy

***d'Cryptor*® SC**

D'CRYPT

Document Number : DC/TER-F01/FIP
Document Version : 1.13
25 May 2017

Configuration Control

Document details

File Name:	SC Non-Proprietary Security Policy v1.13.docx
Document Title:	*d'Cryptor*® SC Cryptographic Module – Non-Proprietary Security Policy
Document Number:	DC/TER-F01/FIP
Document Revision No.:	1.13
Number of pages:	15
Revision Date:	25 May 2017
Remarks	

Contents

1 Scope 4
2 Introduction 4
3 Security Level 4
4 The *d'Cryptor®* SC 5
5 Modes of Operation 7
6 Roles, Identities and Authentication 8
7 Services 10
8 Access Control Policy 11
9 Self-Tests 12
10 Zeroization of CSPs/Cryptographic Keys 12
11 Physical Security Policy 12
12 Mitigation of Other Attacks Policy 14
13 Secure Operation of SC 14
14 Glossary 15

1 Scope

This document contains the specifications for the Security Policy for the *d'Cryptor®* SC (Secure Core) cryptographic module. This information is required in order to satisfy in part the requirements for the validation of the *SC* at level 4 of the FIPS 140-2 standard.

2 Introduction

The *d'Cryptor®* SC cryptographic module is a single-chip (ASIC) hardware security module designed for high security assurance applications. Its bootloader accepts a firmware image after successful authentication, performs a cryptographic verification of the received image, and hands control over to the firmware upon successful verification.

The SC can be employed as a secure cryptographic coprocessor in security modules where it provides a secure operational environment and high-performance cryptographic support. The SC supports a multitude of interfaces, including several UARTs, SPIs, I²C and numerous GPIOs.

The terms "SC", "*d'Cryptor®* SC" and "the module" are used synonymously in this document.

3 Security Level

The SC meets the overall requirements applicable to Level 4 security of FIPS 140-2. Table 1 below shows the individual security level requirement achieved by the module:

Table 1. Security Levels

Security Requirement Area	Level Achieved
Cryptographic Module Specification	4
Cryptographic Module Ports and Interfaces	4
Roles, Services and Authentication	4
Finite State Model	4
Physical Security	4
Operational Environment	N.A.
Cryptographic Key Management	4
EMI/EMC	4
Self-Tests	4
Design Assurance	4
Mitigation of Other Attacks	N.A.

4 The *d'Cryptor*® SC

The *d'Cryptor*® SC is made up of the following components:

Table 2. SC Components

Component	Part Number	Version Number
Base hardware	DC-SPC-1	1.0
d'Cryptor® SC Bootloader (FW)	–	1.2

The principal hardware components of the SC are an ARM-based processor, a 64KB ROM, a 1MB static RAM (SRAM), a 360-byte non-imprinting battery-backed RAM (NI RAM), a 4Kbit one-time programmable (OTP) eFuse memory and a 128-bit battery-backed register, which serves as the tamper log. The SC operates at a clock speed of 500 MHz.

The bootloader performs the boot-up and initialization processes in the SC. It receives and loads an application in the form of a digitally signed firmware image into memory. This firmware image is then verified against its cryptographic signature before control is handed over to it. An SC with a loaded firmware requires a separate validation for it to remain a FIPS 140-2 validated module

4.1 Cryptographic Module Diagram

Figure 1 shows views of the *d'Cryptor*® SC and its cryptographic boundary. Both are indicated by the contiguous dotted red line.

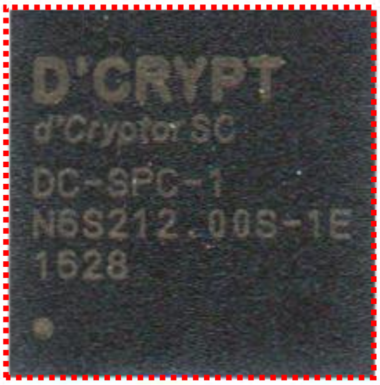

Figure 1. View of *d'Cryptor*® SC

4.2 SC Interfaces

The SC uses the UART0, SPI0 and one GPIO for all communications with the outside world that it performs via service calls. The rest of the interfaces are not used in any way by the SC, but are intended to be used by future applications that may be loaded into the module. The UART0 interface is also known as the *diagnostic port*, as it outputs diagnostic status messages and accepts control commands for activation of services.

The FIPS interface of the SC is made up of all the pins leaving the cryptographic boundary. Table 3 shows the standard logical interfaces and corresponding physical ports on the SC. Each interface has been separated into active and inactive ports. Active ports are those that are used as part of this validation and inactive ports are those that are unused but available once FW is loaded.

Table 3. Mapping of Logical Interfaces to Physical Ports

Logical Interface	Physical Port
Data Input Interface	Active: 3 × SPI0, 3 × GPIO, UART0 Inactive: 3 × SPI1, 4 × SPI2, 5 ×GPIO, I²C, 3 × UART1, 3 × UART2
Data Output Interface	Active: 3 × SPI0, 3 × GPIO, UART0 Inactive: 3 × SPI1, 4 × SPI2, 5 × GPIO, , 2 × I²C, 3 × UART1, 3 × UART2
Control Input Interface	Active: Power-down sense, 4 × External Tamper, 2 × Boot mode , UART0, Reset, 1 × Clock/Crystal input Inactive: 2 × External Tamper, 1 × Clock/Crystal input
Status Output Interface	Active: Tamper Status, Boot Status, Flash Chip Select, UART0, Reset Status, 1 × Crystal output Inactive: 1 × Crystal output
Power Interface	Active: Power supply 7 × 1.1V, 8 × 3.3V, Battery supply 2 × 3.3V, Reservoir 1.1V Inactive: eFuse power 2.5V

4.3 Approved Algorithms

The SC employs two Approved algorithms, as shown in Table 4.

Table 4. List of Approved Algorithms

Algorithm Security Function	Certificate Number	Remarks
ECDSA	859	FIPS PUB 186-4 ▪ DSA with ECC, using NIST Curve P-521 ▪ Signature verification only
SHA	3230	FIPS PUB 180-4 ▪ SHA-512/256 (256-bit hash) – used for OTP memory integrity and module recovery ▪ SHA-512 (512-bit hash) – used together with ECDSA signature verification

4.4 Overview of Security Features

The SC exists in one of two states, operating or non-operating. In non-operating mode, the processor is either not powered or the processor has been rendered non-functional by a security related event such as power-up test failure or physical security mechanism trigger.

The SC ensures that only trusted firmware images can be loaded by requiring all received images to be digitally signed using an ECC 521-bit prime curve digital signature scheme. Upon each power-up, the SC receives a firmware image into its SRAM and verifies the digital signature of the firmware before passing control over to the verified firmware. An SC with a loaded firmware will require a separate validation for it to remain a FIPS 140-2 validated module.

A designated Certificate Authority generates the private and public key pair that is used to sign and verify the received firmware image. The public key (called the Firmware Load Verification Key or "FLVK") is loaded into the OTP memory in the SC as part of the final stage in manufacturing whereas the private key is maintained outside the SC and held securely by the designated entity responsible for generating and signing the firmware images.

The SC supports only a single operator who assumes both the Crypto-Officer and the User roles. Identity-based authentication is employed for the operator to log on to these roles via the Firmware Load service (see Table 7).

The NI RAM is a memory location in the SC where CSPs such as a Key Encryption Key (KEK) can be stored. The NI RAM is backed up via a backup supply that originates in a battery. The source of the backup supply is external to the SC and would be configuration specific. For the purposes of this validation, the NI RAM does not contain any CSPs.

For physical security, the SC implements a tamper mesh to protect the hardware and firmware components as well as any CSP/SPs. The tamper mesh is composed of a metal layer pattern on the topmost layer of the chip, which also provides opacity for the chip. If the mesh is broken, the event is written to the tamper log and the SC stops operating. Attempts to remove or dissolve the tamper mesh will cause the SC to stop operation.

In addition to the tamper mesh, there are six (6) external tamper pins that are monitored for physical tamper. If tamper is detected on any of these six (6) pins, the event is written to the tamper log, and the SC stops operating.

The SC employs Environmental Failure Protection (EFP) features. The module monitors its operating temperature and input voltages. If any of the monitored input voltages, with the exception of battery voltage, fall outside of normal operating range, the SC stops operation. In the event of the operating temperature falling outside of normal operating range or batttery voltage exceeding a prescibed value, the event is written to the tamper log, the NI RAM is cleared and the SC stops operation.

5 Modes of Operation

The SC supports one Approved mode of operation and a non-Approved mode of operation.

In its non-operating state, the SC is either not powered or has been rendered non-functional by a security related event such as a power-up test failure or physical security mechanism trigger.

In its operating state, the SC is either in an Approved or non-Approved mode of operation. The rest of this section assumes that the SC is in an operating state.

When the SC operates in a FIPS 140-2 Approved mode of operation, this is indicated by the following 5-lined message that is displayed via the diagnostic port after powering up (Figure 2):

```
...
Operating mode     = FIPS
ROM integrity      = OK
SHA2-512 BIST      = OK
SHA2-512/256 BIST = OK
ECDSA P-521 BIST   = OK
...
```

Figure 2. Indication of the Approved Mode of Operation

The absence of the messages in Figure 2 is an indication that the SC is not operating in an Approved mode of operation.

The non-Approved mode of operation is used only by the Factory for the purpose of clearing a transient tamper state after a SC has been tampered. The SC is said to enter a transient tamper state when the cause of the tamper is not permanent and can be removed. Some examples of tamper states and their causes are given in Table 5.

Table 5. Tamper Conditions

Source of Tamper	Description of Tamper Cause	Type of Tamper that Resulted
Tamper mesh	Tamper mesh is broken	Non-Transient Tamper
Battery	Battery is removed	Transient Tamper
EFP	One or more of the EFP conditions exceeded the EFP trigger point (Table 11)	Transient Tamper
Tamper Pin(s)	One or more of the Tamper Pins detects a tamper condition	Depends on trigger of tamper source

In addition, if an application firmware image is loaded successfully into the SC, the SC will no longer be operating in a FIPS mode of operation upon execution of the application[1].

6 Roles, Identities and Authentication

The SC provides identity-based authentication to ensure that only an authenticated entity is allowed to operate the SC. It does not support concurrent operators or any maintenance role.

6.1 Identities

The SC supports only a single identity **User** who assumes both the Crypto-Officer and the User roles when operating the module.

[1] If the SC together with the application firmware is revalidated, then the SC will continue to operate in an Approved mode of operation. That however, is outside the scope of the current validation effort.

6.2 Roles

The SC supports the **Crypto-officer/User** (CO/User) role for which an authorized service is available. The module also supports the Factory role, only available in the non-Approved Mode.

6.3 Transition of Roles

The SC always boots up in an “Unauthenticated Role” (UR) state. In this state, no security relevant services can be performed and only unauthenticated services are available.

The SC remains in this state until an operator authenticates to the module by loading a valid firmware image, whereupon it transits into the CO/User role.

6.4 Authentication

The SC employs identity-based authentication. A designated Certificate Authority generates a public and private key pair required for authentication. The public key (the FLVK) is programmed into the OTP memory during the final stage of manufacturing at the factory while the private key is securely retained by the operator of the module.

An operator authenticates to the SC by proving knowledge of the private key. A login request to the SC comes in the form of a firmware signed with the private key. The SC receives this request via either the UART0 or SPI0 interfaces. The SC verifies the firmware’s signature using the FLVK in the OTP memory and upon successful verification, the operator is authenticated to the CO/User role. The Module will only remain in an Approved Mode following successful authentication if the loaded firmware has been validated.

6.4.1 Strength of Authentication

The strength of the authentication mechanism depends on the strength of ECDSA using NIST Curve P-521 with SHA-512, which is approximately 256-bits. The probability that a random attempt at authentication will succeed, which is the probability that a randomly ECDSA P-521 signature can be successfully verified using the public key in the OTP memory, is $1/2^{256}$, which is smaller than the “one in 1,000,000” requirement in FIPS 140-2.

Empirical tests have demonstrated that no more than ten (10) firmware loading/verification can be performed within a one minute period. It follows that the probability that at least one of multiple attempts over a one-minute period will succeed is smaller than “one in 100,000”[2].

There is no feedback of any authentication data to the operator during an authentication session.

6.5 Protection of Authentication Data

The data used in authentication is the FLVK, which is a public key (an SP) that is maintained in the OTP memory while the corresponding private key (CSP) is known only to the operator and not stored in the SC.

The FLVK is programmed into the OTP memory during the final stage of manufacturing at the factory. Once programmed into the OTP memory at the factory, the FLVK cannot be *written* or *modified* by any role.

[2] This probability is “$1 - \text{Prob(all 10 attempts fail)} = 1 - \text{Prob(an attempt fail)}^{10} \approx 1 - (1 - 2^{-256})^{10} \approx 1 - (1 - 10\times2^{-256}) \approx 10\times2^{-256} < 1/100{,}000$.

6.6 Initialization of Authentication Data

During the final stage of manufacturing in the factory, the FLVK is installed into the SC by programming into the OTP memory. This public key is generated by a designated Certificate Authority, along with the private key. The private key is known only to the designated operator to allow them to perform authentication to the required roles.

7 Services

7.1 Authorized Services

There is only one authorized service provided by the SC, namely

- **Firmware Load**

7.1.1 Firmware Load

This service employs two Approved security functions as listed in Table 4, and is used by the bootloader to verify the operator's identity during authentication as well as to verify the authenticity of a firmware image that is loaded via an external source.

7.2 Unauthenticated Services

The SC supports the following unauthenticated services:

- **Show Status**
- **Perform Self-Tests**

7.2.1 Show Status

The current status of the SC can be obtained by performing the **Show Status** service. This service can be activated in two ways, namely:

- Measure the state of the Boot Status GPIO pin
- Monitor the output of the diagnostic port (UART0)

The state of the Boot Status GPIO pin indicates whether or not a firmware has been loaded into the SC (i.e., LOADED or NOT_LOADED). The diagnostic port displays text messages that provide the same indication.

7.2.2 Perform Self-Tests

The power-up self-tests can be initiated by power cycling the module. The results of these self-tests can be observed via the diagnostic port.

7.3 Non-Approved Services

The SC supports one non-Approved service that is used only in the non-Approved mode of operation.

- **Module Recovery**

7.3.1 Module Recovery

This service allows the Factory to reinstate a tampered but operational SC into a state whereby it can operate in an Approved mode of operation. This is done by clearing the tamper status in the SC while the module is powered.

The module can only be recovered if the tamper condition no longer exists. If the Module Recovery service is executed and the tamper is still present, the module will immediately re-enter the tamper state.

Note that the execution of this service does not compromise the security of the module in any way because its function is limited to transient events (see Table 5) such as detections of an unacceptable voltage or temperature range. A more serious tamper event would cause the module to immediately re-enter the tamper state, show tamper evidence, and/or cause power on self-tests to fail.

8 Access Control Policy

8.1 List of CSPs

There are no CSPs stored in the SC.

8.2 Security Parameter

The Security Parameter (SP) in the SC is listed in Table 6.

Table 6. Security Parameter in the SC

SP	Description
FLVK	Firmware Load Verification Key – ECDSA P-521 Public key stored in the OTP memory. Used by the SC to authenticate the **CO**/**User**, as well as verify the signature of a firmware image that is loaded into the SC.

8.3 Roles and Services

The relationship between roles and services and the types of access services they have to the SP is summarized in Table 7. The access types are explained as follows:

- **R** (*"read*") – The SP can be read out by the service.
- **X** (*"execute*") – The SP is used by the service.

Table 7. Roles vs. Services and Access Types to SP

Service	Description	UR	CO/ USR	Factory	SP	CSP	Access Type
Firmware Load	Loads an external firmware image	✘	✓	✘	FLVK	–	R, X
Show Status	Shows module status	✓	✓	✓	–	–	–
Perform Self-Tests	Perform power-up self-tests	✓	✓	✓	–	–	–
Module Recovery	Recover module from tamper	✘	✘	✓	–	–	–

Notes: "✓" is "allowable" "✗" is "unallowable" "–" is "not applicable"

"UR" means "Unauthenticated Role"

9 Self-Tests

The SC performs a series of self-tests during power-up to ensure that all the cryptographic operations it provides are functioning properly.

If any of the self-tests (other than the Firmware Load Test) fails, the SC immediately halts, thus leaving the SC in an unusable state and requiring a return of the module to the factory for recovery.

9.1 Power-Up Self-Tests

The power-up self-tests consists of the following tests, shown in Table 8:

Table 8. Power-Up Self-Tests

Self-Test	Description
Cryptographic Algorithm Tests	Known-answer test for all cryptographic algorithms implemented in SC: ▪ Verify : ECDSA (NIST Curve P-521) ▪ Message digest : SHA-512 and SHA-512/256
Firmware Integrity Test	Bootloader: 32-bit Cyclic Redundancy Check (CRC) eFuse: SHA-512/256 verification over contents of eFuse

9.2 Conditional Self-Tests

The conditional self-tests comprises the following test, shown in Table 9:

Table 9. Conditional Self-Tests

Self-Test	Description
Firmware Load Test	ECDSA signature verification using NIST Curve P-521

10 Zeroization of CSPs/Cryptographic Keys

The SC does not contain any CSPs and hence it is not necessary for the module to perform zeroization of CSPs or cryptographic keys.

11 Physical Security Policy

11.1 Physical Embodiment

The SC is a single-chip (ASIC) cryptographic module.

11.2 Physical Security Mechanisms

The SC uses standard production-quality components that meet typical commercial-grade specifications.

The ASIC is protected with a tamper mesh. The tamper mesh is composed of a metal layer pattern on the topmost layer of the chip. If the mesh is broken, the event is written to the tamper log and the module stops functioning. Attempts to remove or dissolve the tamper mesh will also cause the SC to stop functioning.

In addition to the tamper mesh, there are six (6) external tamper pins that are monitored for physical tamper. If tamper is detected on any of these six (6) pins, the event is written to the tamper log and the SC stops operating.

11.3 Environmental Failure Protection (EFP)

The SC employs environmental failure protection features that protect it from environmental conditions outside of its normal operating ranges by monitoring its operating temperature and input voltages and taking appropriate action when unusual environmental conditions are detected.

The normal operating ranges of the SC are indicated in Table 10.

Table 10. Normal Operating Ranges

Environmental Condition	Normal Operating Range
Temperature	0 ºC - 85 ºC
IO Power Supply	3.1 V – 3.5 V
Analog Power Supply	3.1 V – 3.5 V
Core Power Supply	1.04 V – 1.16 V
Battery Power Supply	2.7 V – 3.5 V

The SC stops operation when any of the following conditions are met:

Table 11. EFP Trigger Points

Environmental Condition	Below	Above
Temperature	– 15 ºC ± 10 ºC	115 ºC ± 10 ºC
IO Power Supply	2.3 V – 2.9 V	3.5 V – 4.1 V
Analog Power Supply	2.3 V – 2.9 V	3.5 V – 4.1 V
Core Power Supply	0.7 V – 1.0 V	1.16 V – 1.6 V
Battery Power Supply	1.6 V – 2.5 V *	3.5 V – 4.1 V

* *Only applicable if all the other three (3) main power supplies are not active (i.e. zero voltage).*

In addition to the above, in the event that

- the operating temperature falls outside the normal operating range and reaches a triggering point within the range specified in Table 11, or
- the battery voltage exceeds the higher bound of the normal operating range and reaches a triggering point within the range specified in Table 11,

the event is written to the tamper log and the SC stops operation.

11.4 Physical Security Checks

The following physical check on the SC should be carried out periodically to ensure that physical security is maintained:

- Inspect exposed surfaces of the module for any signs of physical tamper. Such signs might include deep scratches or any irregularity on the surface of the chip.

It should be noted that the interval between inspections would depend on the application that the SC is used for, as well as the security threat that the SC is exposed to under its operational environment. It is recommended that examination of the module surface be carried out at least once every 6 months.

It is important to note that activating the tamper detection and response as described in Sections 11.2 and 11.3 causes the module to stop functioning and thereafter necessitates the return of the module to the factory for recovery.

12 Mitigation of Other Attacks Policy

The SC is not designed to mitigate any specific attacks.

13 Secure Operation of SC

13.1 Factory Defaults

A *d'Cryptor*® SC is delivered from the factory in an Approved mode of operation, pre-installed with *d'Cryptor*® SC Bootloader (with version indicated in Table 2), and initialized with one ECDSA public key (FLVK).

13.2 Operating the SC

The SC operates in an Approved mode of operation when it is shipped from the factory. This can be determined by powering up the SC and observing the approved mode of operation indicator as described in Section 5. It is also important to verify that the chip marking on the module is as shown in Figure 1.

The **Firmware Load** service loads an application firmware image from one of three possible sources that depends on the boot mode. The operator configures the boot mode (before powering up the SC) by setting the values of the two boot mode control input pins as follows:

Table 12. Boot Mode Selection

Boot Mode	Boot0 Pin	Boot1 Pin	Description
UART	Low	Low	Firmware is loaded via UART0
SPI	High	Low	Firmware is loaded via SPI0
FLASH	Low	High	Firmware is loaded via SPI0 Flash

Before activating any cryptographic service, the operator would have to authenticate into an authorized role by logging on into the CO/User role.

13.3 Security Rules

13.3.1 Operational Security Policy

- A proper operational Security Policy should be in place that requires the FLSK (the private key counterpart of FLVK) to be kept under lock and key, and known only to the entity or personnel who is authorized to authenticate into the CO/User role.
- The validated module does not allow entry or output of keys.
- Once a module is tampered, the operator should immediately return it to the factory for recovery.

13.3.2 Authentication Security Rules

Authorized logins are subjected to the following rules:

- Identity-based authentication is used to logon to an authorized role.
- The module accepts only one role to be logged on at any time. No concurrent logon is allowed.

14 Glossary

14.1 Acronyms

FLSK	Firmware Load Signing Key
FLVK	Firmware Load Verification Key
CSP	Critical Security Parameter(s)
EFP	Environmental Failure Protection
FIPS	Federal Information Processing Standards
GPIO	General-Purpose Input/Output
KEK	Key-Encryption Key
SC	Secure Core Cryptographic Module
SP	Security Parameter(s)
SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver/Transmitter

14.2 Definitions

mode of operation The mode in which the SC is operating. The SC always operates in *FIPS mode* (which is the *Approved mode of operation*).

security parameter Security-related information (e.g. public cryptographic keys) whose modification can compromise the security of a cryptographic module. Note the distinction between *SP* and *CSP*. The *disclosure* of a SP does not affect the security of the module.